PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN NIRKABEL DARI SERANGAN DDOS (*DISTRIBUTED DENIAL OF SERVICE*) BERBASIS *HONEYPOT*

Sutarti[1], *Khairunnisa*[2]
Program Studi Sistem Komputer Fakultas Teknologi Informasi Universitas Serang Raya
sutarti86@gmail.com[1], **anirakhairunnisa@gmail.com**[2]

Abstrak - Masalah keamanan komputer merupakan faktor yang sangat penting untuk diperhatikan dan dikelola dengan baik oleh sistem administrator, banyak sekali cara yang ditempuh untuk menghalangi seseorang/perusahaan untuk dapat memberikan layanan yang optimal. Namun seringnya jaringan *server* mengalami gangguan karena diserang yang disebabkan oleh serangan jenis DDoS, gangguan tersebut bisa berupa kegagalan sistem, *halt, error request* bahkan kerusakan *hardware server*. Hal inilah yang terjadi di ruang *server* PDAM Tirta AlBantani. Dengan membuat sistem keamanan jaringan *server* menjadi aman dari serangan DDoS, sistem *honeypot* memberikan keamanan bagi *server* agar tidak adanya penyerangan dari DDoS. Sehingga dengan diterapkannya sistem *honeypot*, dengan membuat satu *server* sebagai korban dengan membangun sistem *honeypot* komputer *server* dan keamanan jaringan yang lain akan terlindungi, karena penyerang melihat target seolah-olah itu adalah OS target yang bisa diserang, padahal itu adalah sistem *honeypot* yang sengaja dibuat untuk menampung dan meladeni penyerang. Tentunya dengan sistem ini, dapat meningkatkan keamanan jaringan *wireless*, dan dapat melindung *server* dari gangguan serangan jenis apapun termasuk jenis serangan DDoS.

Kata Kunci : DDoS, *Honeypot, Security Network, Server*

I. PENDAHULUAN

Kebutuhan akan teknologi informasi di era modern ini sangat besar serta dapat diaplikasikan dalam berbagai bidang, sebab itu juga banyak pihak-pihak yang saat ini jadi bergantung pada sistem komputer sehingga sistem komputer dituntut untuk berjalan sepanjang waktu pada jaringan internet.

PDAM Tirta Al Bantani merupakan perusahaan daerah air minum milik negara, di mana saat ini telah berkembang demikian pesat dan mulai meningkatkan peralihan teknologi dari manual menjadi digital. Seiring perkembangan teknologi digital itu sendiri, maka akan banyak rintangan dan permasalahan yang akan dihadapi. Salah satu kendala yang akan dihadapi adalah di bidang teknologi informasi. Satu di antara tantangan itu adalah sistem keamanan. Sistem keamanan jaringan komputer bisa jadi secara fisik maupun secara non fisik.

Secara fisik adalah sistem keamanan *server* beserta perangkat pendukungnya dari pencurian, bencana alam dan kerusakan akibat kesalahan manusia. Sedangkan secara non fisik adalah berupa kerusakan sistem operasi *server*, kerusakan pada program aplikasi ataupun terhadap gangguan dari luar sistem seperti serangan *hacker*, *virus*, *trojan* dan lain sebagainya.

Administrator *server* seringkali mengabaikan aspek-aspek keamanan yang secara umum telah diketahui memiliki celah-celah untuk disusupi. Di antara kelalaian yang terjadi adalah seorang administrator *server* kurang memperhitungkan efek samping terhadap aplikasi-aplikasi yang di-*install* pada *web server* yang dikelolanya. Pada prinsipnya sebagian besar aplikasi tersebut memang diperlukan untuk mempermudah pekerjaan, namun saat sebuah program aplikasi di-*install* maka program tersebut akan membuka sebuah *port* atau beberapa *port* yang dibutuhkan untuk berkomunikasi dengan dunia luar. *Port* yang terbuka tersebut kemudian menjadi jalan bagi program jahat untuk masuk dan menyusup ke dalam sistem komputer.

Lemahnya sistem keamanan yang diterapkan oleh PDAM Tirta Al Bantani dari serangan DDoS (*Distributed Denial of Service*). Serangan yang mengakibatkan sistem keamanan jaringan diserang mengalami gangguan. Gangguan tersebut bisa berupa kegagalan sistem, *halt*, *error* request bahkan kerusakan *hardware server* tersebut. Setelah melihat masalah-masalah pada sistem keamanan jaringan di lingkungan PDAM Tirta Al Bantani maka dibutuhkan suatu sistem untuk melindungi komputer *server*. Karena begitu merugikannya serangan DDoS terhadap suatu *server* maka diperlukan sebuah solusi untuk menyelesaikan permasalahan tersebut, *honeypot* menjadi salah satu solusi untuk mendeteksi serangan DDoS. *Honeypot* adalah suatu sistem yang didesain untuk diserang dan disusupi oleh *cracker*, oleh karena itu semua trafik yang menuju *honeypot* patut dicurigai sebagai aktivitas penyusupan. *Honeypot* dapat digunakan untuk membantu administrator jaringan untuk mendeteksi trafik berbahaya.

II. LANDASAN TEORI

2.1 Kajian Pustaka

Penelitian ini dilakukan berdasarkan penelitian-penelitian yang pernah dilakukan sebelumnya, di antaranya yaitu penelitian yang dilakukan oleh Mentang dkk (2015), penelitian ini menyatakan bahwa dengan menggunakan metode WIDS mampu mendeteksi serangan DoS (*Denial of Service*). Penulis melakukan penerapan pada sistem operasi Linux menggunakan

snort sebagai mesin sensor dan *IP tables* sebagai penanganan serangan dapat menjadi solusi keamanan jaringan nirkabel dari serangan yang mengancam. Konfigurasi sistem dibangun dalam jaringan WAN (*Wide Area Network*) yang dirancang untuk merepresentasikan pengujian. Hasil analisis dari setiap pengujian yang dilakukan menyimpulkan bahwa setiap tindakan yang dilakukan oleh penyerang terhadap jaringan dapat diketahui, sehingga dapat dilakukan penanganan sebelum terjadi kerusakan lebih luas.

Penelitian yang dilakukan oleh Zulkarnaen (2010), keamanan jaringan yang digunakan pada KPPBC Palembang masih bersifat standar. KPPBC Palembang pernah mengalami pencurian data pada Tahun 2008. Data yang diberikan ke pihak lain untuk keperluan tertentu sering diketahui oleh pihak lain dan setelah ditelusuri bentuk serangan yang dilakukan pihak lain adalah usaha penyadapan dengan menggunakan program Nmap dan serta berusaha untuk masuk ke *port* yang terbuka. Gangguan keamanan komputer yang dialami KPPBC Palembang digolongkan dalam aspek privat (*privacy/confidentiality*). KPPBC Palembang masih memanfaatkan sistem keamanan melalui *firewall* dan *anti spyware*. Hal ini belum dapat mengatasi sabotase/pencurian data yang dilakukan oleh pihak tertentu karena tidak dapat menemukan pelaku penyerangan. Penelitian yang dilakukan oleh Ferdiansyah (2013), tingkat ketersediaan (*availability*) data merupakan hal mutlak yang harus disediakan oleh pihak penyedia data/informasi. Apa yang dibutuhkan oleh pengguna layanan IT harus dapat dipenuhi, sehingga tingkat ketersediaan (*availability*) ini merupakan salah satu faktor yang harus diperhatikan dalam mencapai tingkat dari keamanan informasi. *Honeypot* merupakan sebuah teknologi yang bertindak sebagai umpan sehingga penyerang terjebak dalam melakukan serangannya. Hal ini dapat diilustrasikan bahwa *honeypot* akan membuat *server* bayangan/palsu (*fake*) sebagai umpan. Setiap pergerakan dari jenis-jenis serangan tersebut dapat dipantau dan dianalisis hasilnya. Hasil akhir dari penelitian ini merupakan sebuah kebutuhan (*requirement*) teknologi *honeypot* yang sesuai dengan kondisi di Jurusan Teknik Informatika UNPAS.

Prasetyo dkk (2011), permasalahan yang diangkat adalah kejahatan di dunia internet yang dikenal dengan *cybercrime* telah banyak menimbulkan kerugian dan pembobolan data sepanjang tahun. Metode yang digunakan adalah IDS yang akan dikolaborasikan dengan *honeypot*, di mana honeypot merupakan sistem yang dibuat menyerupai sistem aslinya untuk melakukan korelasi *alert* yang dihasilkan oleh masing-masing sensor (IDS dan *Honeypot*). Hasilnya sistem *server* terlindungi dan para penyusup dapat dialihkan ke *server* palsu dan data di *server* asli lebih aman. Maka kesimpulannya *honeypot* dapat dikolaborasikan dengan beberapa sistem deteksi.

Keamanan Jaringan Komputer

Menurut Ariyus (2007: 3) "Keamanan jaringan secara umum adalah komputer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar daripada komputer yang tidak terhubung ke mana-mana." Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun *network security* biasanya bertentangan dengan *network access*, di mana bila *network access* semakin mudah, maka *network security* semakin rawan, begitu pula sebaliknya.

Keamanan jaringan (*network security*) dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan.

Menurut Dewananta (2007), prinsip keamanan jaringan komputer diklasifikasikan menjadi 3 bagian:

1. *Confidentiality* (kerahasiaan)
2. *Integrity* (integritas)
3. *Availability* (ketersediaan)

Ancaman

Menurut Utomo (2006: 111) pada dasarnya ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer. Oleh karena itu, harus ditentukan siapa saja yang diperbolehkan mempunyai akses legal ke dalam sistem, dan ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan sangat berguna apabila dapat membedakan tujuan-tujuan tersebut pada saat merencanakan sistem keamanan jaringan komputer. Beberapa tujuan para penyusup adalah:

1. Pada dasarnya hanya ingin tahu sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut dengan *the curius*.
2. Membuat sistem jaringan menjadi *down*, atau mengubah tampilan situs *web*. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai *the malicious*.
3. Berusaha untuk menggunakan sumber daya di dalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup seperti ini sering disebut sebagai *the high-profile intruder*.
4. Ingin tahu data apa saja yang ada di dalam jaringan komputer untuk selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini sering disebut sebagai *the competition*.

Menurut Utomo (2006: 129) ada beberapa jenis ancaman yang dapat terjadi pada keamanan jaringan komputer antara lain sebagai berikut:

1. *Packet sniffing*

   Packet sniffing adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun nirkabel. Prinsip dasar pencurian jenis ini adalah bahwa semua koneksi *ethernet* adalah koneksi yang bersifat *broadcast*, di mana semua *host* dalam sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah *host*. Pada keadaan normal hanya *host* yang menjadi tujuan paket yang dikirimkan dan

akan memproses paket tersebut sedangkan *host* yang lain akan mengacuhkan paket-paket tersebut. Namun pada keadaan tertentu, sebuah *host* dapat mengubah konfigurasi sehingga *host* tersebut akan memproses semua paket yang dikirimkan oleh *host* lain.

2. *IP spoofing*
   Adalah model serangan yang bertujuan untuk menipu seseorang. Serangan ini dilakukan dengan cara mengubah alamat asal sebuah paket sehingga dapat melewati *firewall* yang telah dipasang. Pada dasarnya alamat IP asal sebuah paket dituliskan oleh sistem operasi host yang mengirimkan paket tersebut. Dengan melakukan *raw-socket-programming*, seseorang dapat menuliskan isi paket yang akan dikirimkan setiap bit-nya sehingga dapat melakukan pemalsuan data.
3. *DNS Forgery*
   Yaitu melakukan penipuan data-data DNS. Cara kerja dari DNS adalah sederhana yaitu sebuah *host* mengirimkan paket (biasanya dengan tipe UDP) yang pada *header* paket tersebut berisikan alamat *host* penanya, alamat DNS *resolver*, pertanyaan yang diinginkan dan sebuah nomor identitas.
4. *DNS Cache Poisioning*
   Bentuk serangan lain dengan menggunakan data DNS adalah *DNS Cache Poisioning*. Metode ini dengan memanfaatkan *cache* dari setiap *server* DNS yang merupakan tempat penyimpanan sementara data-data domain yang bukan tanggung jawab *server* DNS tersebut.
5. *Worm*
   Merupakan program yang menyebar sendiri dengan cara mengirimkan dirinya sendiri ke sistem. *Worm* tidak akan menyisipkan dirinya ke obyek lain. Penyebaran *worm* saat ini banyak disebabkan karena pengguna tidak melakukan *update* terhadap aplikasi *software* yang digunakan.
6. Virus
   Merupakan program yang dapat menyisipkan dirinya ke obyek lainnya seperti pada *file executable (.exe)* dan beberapa jenis dokumen yang sering digunakan (seperti .doc).
7. DoS/DDoS

Merupakan bentuk serangan pada jaringan komputer yang berusaha untuk menghabiskan sumber daya sebuah peralatan komputer sehingga jaringan komputer menjadi terganggu. Proses awal koneksi dengan menggunakan protokol TCP/IP adalah *three way handshake*. Proses ini dimulai pada saat klien mengirimkan paket dengan tanda SYN, kemudian pihak *server* akan menjawab dengan mengirimkan tanda SYN dan ACK dan pihak klien akan kembali mengirimkan dengan tanda ACK. Ketika koneksi sudah terbuka sampai salah satu pihak mengirimkan paket FIN atau RST terjadi *connection time-out*. Selain terjadi inisiasi koneksi, juga terjadi pertukaran data parameter agar koneksi dapat berjalan dengan baik.

Honeypot

Menurut Spitzner (2003*)* *honeypot* merupakan salah satu jenis teknologi terbaru di bidang keamanan sistem dan jaringan komputer yang digunakan sebagai pelengkap teknologi keamanan sebelumnya. Teknologi keamanan sebelumnya seperti *Firewall* dan IDS merupakan teknologi konvensional di mana sistem pertahanan dibangun untuk mencegah penyerang menembus masuk ke dalam area yang dilindungi.

Dalam bahasa sederhana, *honeypot* adalah sistem atau komputer yang sengaja dikorbankan untuk menjadi target serangan *hacker*. Oleh sebab itu setiap interaksi dengan *honeypot* patut diduga sebagai aktivitas penyusupan. Misal, jika ada orang yang melakukan *scanning* jaringan untuk mencari komputer yang *vulnerable* (rentan), saat ia mencoba koneksi ke *honeypot* tersebut, maka *honeypot* akan mendeteksi dan mencatatnya, karena seharusnya tidak ada *user* yang berinteraksi dengan *honeypot*. Keunggulan *hacker* adalah anonimitas. *Honeypot* merupakan senjata orang-orang baik yang membuat situasi menjadi lebih imbang. Tidak seperti IDS atau *firewall*, *honeypot* tidak menyelesaikan suatu masalah tertentu, tetapi memiliki kontribusi terhadap keseluruhan keamanan (Spitzner, 2003).

III. METODE PENELITIAN

Jaringan *server* di PDAM Tirta AlBantani menerapkan sistem keamanan jenis *firewall*. Setiap mengalami gangguan keamanan jaringan *server* yang dialami PDAM digolongkan dalam aspek privat (*privacy/confidentiality*). Hal ini belum dapat mengatasi sabotase/pencurian data yang dilakukan oleh pihak tertentu karena tidak dapat menemukan pelaku penyerang.

Gangguan pada sistem dapat terjadi karena faktor ketidaksengajaan yang dilakukan oleh pengelola (*human error*), akan tetapi tidak sedikit pula yang disebabkan oleh pihak ketiga. Gangguan dapat berupa perusakan, penyusupan, pencurian hak akses, penyalahgunaan data maupun sistem, sampai tindakan kriminal melalui aplikasi jaringan komputer.

Dalam melakukan persiapan fungsi sistem hendaknya disiapkan pengamanan dalam bentuk berikut:

1. Mengelompokkan terminal yang difungsikan sebagai pengendali jaringan atau titik pusat akses (*server*) pada suatu jaringan, yang selanjutnya harus diberikan pengamanan secara khusus.
2. Menyediakan pengamanan fisik berupa ruangan khusus untuk pengamanan perangkat yang disebut pada *point* nomor 1. Ruangan tersebut dapat diberikan label NOC (*Network Operating Center*) dengan membatasi personil yang diperbolehkan masuk.
3. Memisahkan sumber daya listrik untuk NOC dari pemakaian yang lain, perlu juga difungsikan UPS (*Uninteruptable Power Supply*) dan *Stabilizer* untuk menjaga kestabilan *supply* listrik yang diperlukan perangkat pada NOC.

4. Merapikan ruangan dan memberikan label serta pengklasifikasian kabel.
5. Memberikan *soft security* berupa sistem *firewall* pada perangkat yang difungsikan di jaringan. Merencanakan *maintenance* dan menyiapkan *Back Up* sistem.

Spesifikasi *Hardware*

Spesifikasi dari perangkat keras dari jaringan sudah cukup baik, komponen-komponen perangkat keras sudah sesuai dengan standar.

1. *Modem*
2. *Hub*
3. *Switch*
4. *Mikrotik*
5. Kabel UTP
6. *Access Point*
7. *USB Wireless*
8. *Printer* Epson

Spesifikasi *Software*

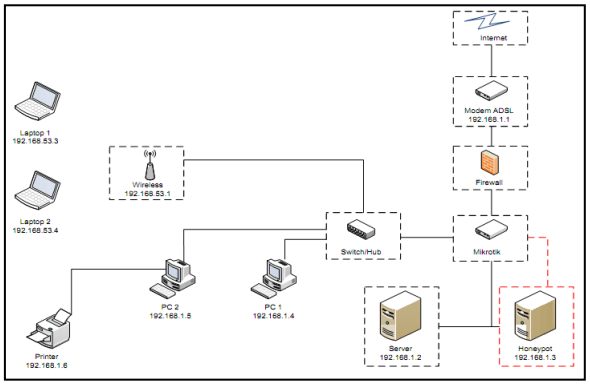
Software atau sistem operasi dari perangkat yang digunakan para pengguna cukup bervariasi.

1. Ubuntu
2. Nmap
3. Winbox
4. Apache
5. MySQL

IV. HASIL DAN PEMBAHASAN

Topologi Jaringan

Untuk dapat mengimplementasikan teknologi sistem keamanan *honeypot*, terlebih dahulu harus dipahami tentang arsitektur dasarnya.

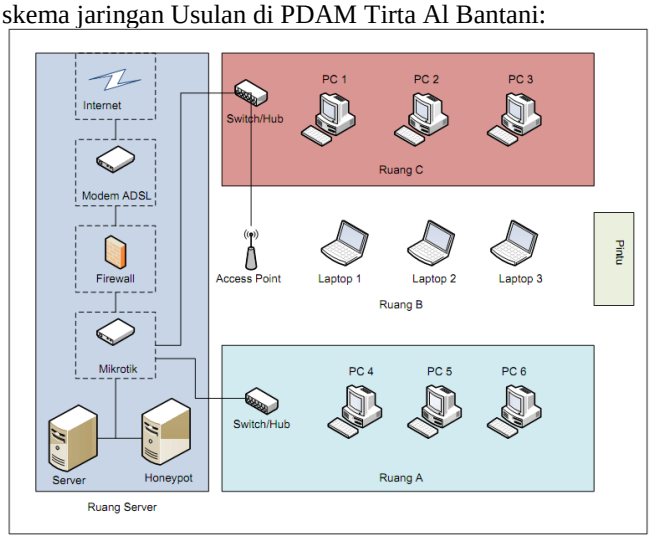


Sumber: Dokumen Pribadi

Gambar 1. Topologi Jaringan Usulan Menggunakan *Honeypot*

Skema Jaringan

Berisi tentang gambar rangkaian jaringan komputer pada obyek penelitian dan spesifikasi jaringan komputer yang ada pada obyek penelitian secara detail (gambar skema jaringan dapat berasal dari perusahaan atau dibuat menggunakan aplikasi visio atau aplikasi sejenis), dengan menggunakan skema jaringan usulan wifi penggunaan *hub* dapat dikurangi, efisien dan lebih cepat. Di bawah ini adalah skema jaringan Usulan di PDAM Tirta Al Bantani:



Sumber: Dokumen Pribadi

Gambar 2. Skema Jaringan Usulan PDAM Tirta Al Bantani

Instalasi *Dionaea Honeypot*

Dionaea adalah salah satu *low interaction honeypot* yang menawarkan layanan SMB, HTTP, FTP dan TFTP.

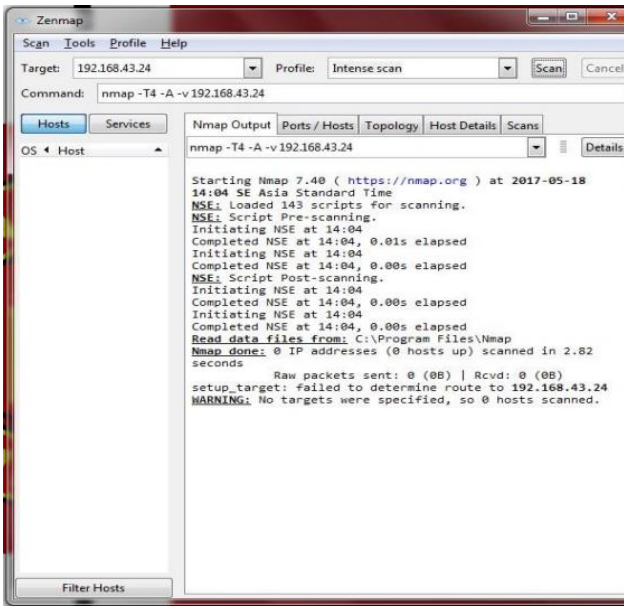
1. Sebelum melakukan konfigurasi, beberapa paket berikut ini sudah ter-*install* yaitu Liblcfg, Libemu, Libnl, Libev, Python 3.2, Cython, Libcurl, Libpcap.
2. Untuk *install* dionaea, input dua baris *repository* berikut ke dalam *sources.list*, ketik di terminal.
   Nano /etc/apt/sources.list.
   Kemudian *copy source* di bawah ini.
   Deb http://ppa.launchpad.net/honeynet/nightly/ubuntu precise main.
   deb-src http://ppa.launchpad.net/honeynet/nightly/ubuntu precise main.
3. *Update* dan *install* dionaea.
   Sudo apt-get update.
   Sudo apt-get install dionaea.
4. *Set up directories* yang dapat diakses oleh dionaea:
   Sudo mkdir –p /var/dionaea/wwwroot.
   Sudo mkdir –p /var/dionaea/binaries.
   Sudo mkdir –p /var/dionaea/log.
   Sudo chown –R nobody:nogroup /var/dionaea.
5. Update file config dengan direktori-direktori yang baru:
   Sudo mv /etc/dionaea/dionaea.conf.dist /etc/dionaea/dionaea.conf
   Sudo sed –i ‘s/var\/dionaea\///g’ /etc/dionaea/dionaea.conf
   Sudo sed –i ‘s/log\/\/var/dionaea\log\//g’ /etc/dionaea/dionaea.conf
6. Sebelum memulai dionaea, konfigurasi *file* yang ada

di/etc/dionaea/dionaea.conf. Lalu *edit logging* untuk mengurangi jumlah *logging*. Set *levels* dari "*all*" ke *warning*, *error*.
Aktifkan Dionaea sebagai Daemon
sudo dionaea -c /etc/dionaea/dionaea.conf -w /var/dionaea -u nobody -g nogroup –D

7. Selanjutnya cek proses dionaea: ps -ef | grep dionaea.
8. Cek status jaringan: netstat -tnlp | grep dionaea
9. Untuk melihat *log*, cek di sini:
   Cd /var/dionaea/log.
10. *Fingerprinting* dengan p0f
    Untuk lebih jelas tentang penyerangan dan sistem operasi dan versinya, perlu meng-*install library fingerprinting* "p0f". Untuk meng-*install*-nya jalankan perintah berikut: Sudo apt-get install p0f.
11. Edit /etc/dionaea/dionaea.conf pada bagian ihandler. Hilangkan comment untuk "p0f".
12. Dionaea memiliki p0f yang sudah dimasukkan stream analysis, namun p0f harus pre-autorisasi dan dijalankan secara terpisah. sudo p0f -i any -u root -Q /tmp/p0f.sock -q -l -d -o /var/dionaea/p0flog.log
13. Jalankan kembali Dionaea:
    Sudo dionaea –c /etc/dionaea/dionaea.conf –w/var/dionaea –u nobody –g nogroup –D
14. Menguji proses p0f berjalan sebelum konfigurasi socket yang terkait dengan /tmp/p0f.sock, kemudian Dionaea: Ps –ef | grep p0f.

Pengujian sistem keamanan jaringan awal

Sistem keamanan jaringan awal (*firewall*) adalah sistem keamanan jaringan yang meliputi gangguan serangan jenis DDoS (*Distributed Denial of Service*), yang dapat mengakibatkan kegagalan sistem atau kerusakan *hardware server*.



Sumber: Dokumen Pribadi

Gambar 3. Paket serangan *port scanning* (nmap)

Pengujian pertama adalah kondisi sebuah *server* layanan tanpa menggunakan sistem *honeypot*. Pada pengujian ini, sistem pencegahan penyusupan dalam keadaan normal yaitu tidak ada paket data yang dikirim berupa serangan *port scanning* dan DOS.

Hasil dari pengujian setelah adanya serangan dapat dilihat pada Gambar 4.

Sumber: Dokumen Pribadi

Gambar 4. Hasil pengujian setelah adanya serangan

Dari hasil pada Gambar 4. *server* terjadi *bluescreen* akibat dari serangan DoS. Sehingga layanan yang diberikan oleh *server* menjadi terganggu.

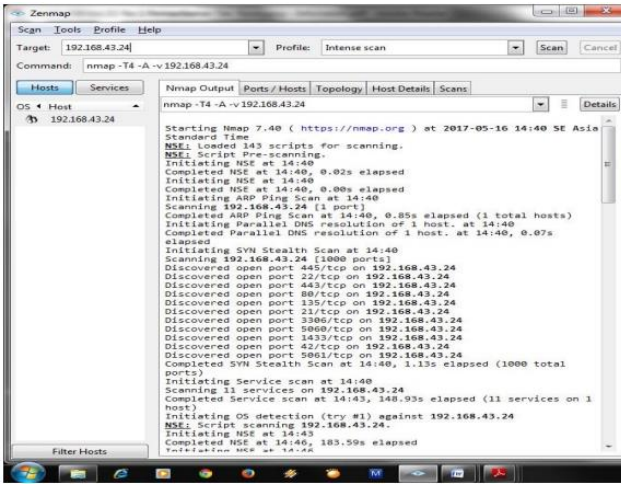
Tabel 1. Pengujian Jaringan Awal Sistem Keamanan *Firewall*

No	OS	Proses *Running*		Keterangan
		Berhasil Masuk	Gagal Masuk	
1	*Spam*	√		Masih banyak celah di *firewall* yang menyebabkan *spam* bisa masuk ke jaringan
2	*Malware*	√		Terbukanya *port* di IP publik menyebabkan penyerang bisa masuk ke jaringan dan menyimpan *malware* di *server*.
3	*DdoS Attack*	√		Terbukanya *port* dan lemahnya *firewall* yang menyebabkan *server* dengan sangat mudah dibobol oleh penyerang.
4	*Scammer*	√		IP Publik yang dilindungi memudahkan penyerang men *scan* IP dan melancarkan serangan.
5	*Virus*	√		Sudah hancurnya sistem keamanan memudahkan penyerang menyimpan virus di komputer *server*.

Sumber: Dokumen Pribadi

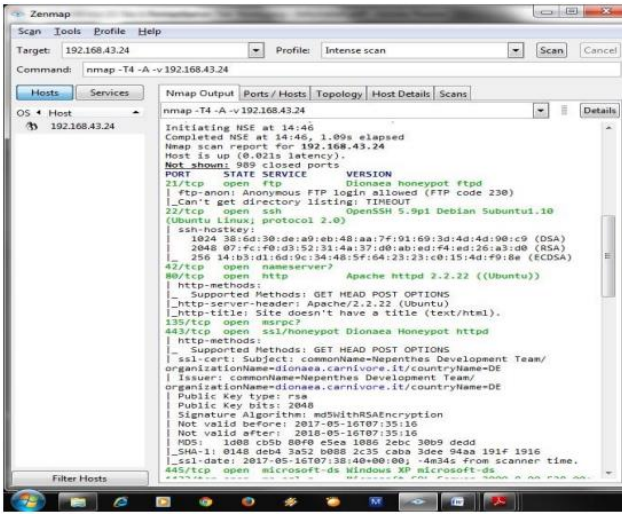
Pengujian Sistem Keamanan Jaringan Akhir

Sistem keamanan jaringan baru adalah sistem keamanan jaringan berbasis honeypot. Pada pengujian kedua, penelitian ini menggunakan sistem *honeypot*. *Honeypot* sudah dikonfigurasi terlebih dahulu dan dipasang di depan *server*. Pada pengujian ini, serangan berupa *port scanning* dan DOS langsung menuju *server* tanpa adanya pencegahan penyusupan.



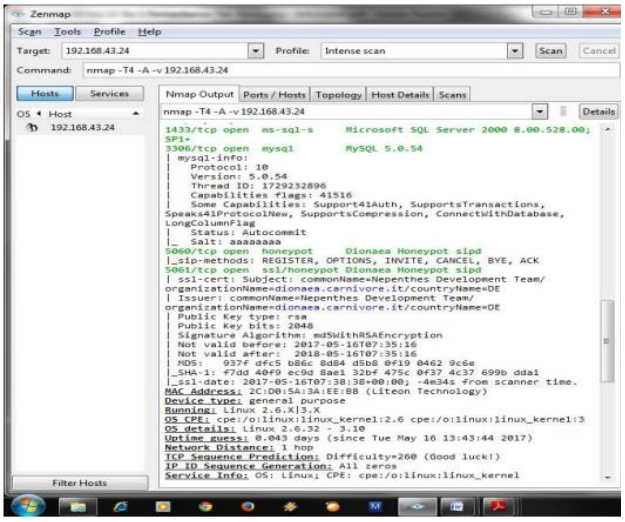
Sumber: Dokumen pribadi

Gambar 5. Paket Serangan *Port Scanning* (nmap)



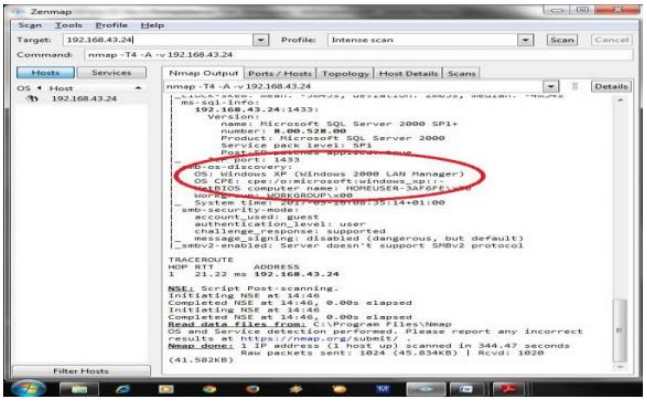
Sumber: Dokumen Pribadi

Gambar 6. Tampilan Paket Serangan *Port Scanning*



Sumber: Dokumen Pribadi

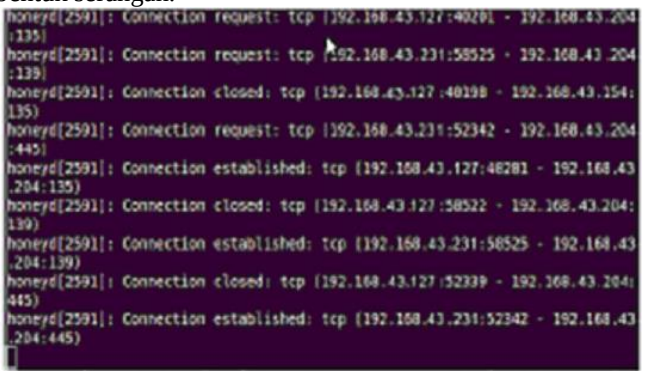
Gambar 7. Tampilan Paket Serangan *Port Scanning*



Sumber: Dokumen Pribadi

Gambar 8. Tampilan Paket Serangan Port Scanning

Serangan *Port Scanning* dibangkitkan oleh nmap berupa Zenmap pada client 2 dengan IP 192.168.43.24, pada Gambar 8 memperlihatkan bahwa client 2 telah mengirimkan paket serangan. Setelah serangan dikirim, *snort* di *server* mengeluarkan *alert* bahwa IP 192.168.43.24 melakukan serangan berupa *Port Scanning* (nmap) yang dapat dilihat pada Gambar 9 yang terdiri dari IP penyerang, IP yang diserang dan bentuk serangan.



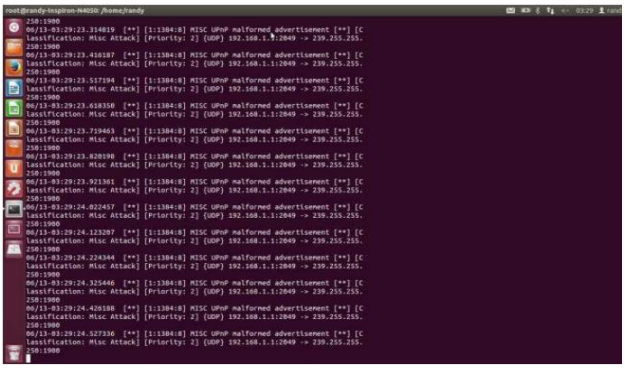
Sumber: Dokumen Pribadi

Gambar 9. Aktifitas Serangan pada *Honeyd*

Pada *Honeyd* (*server* palsu) akan menampilkan aktifitas serangan yang terdiri IP serangan *port scanning* dan IP DoS. Pembelokan serangan pada *server* palsu, tidak memberikan kecurigaan pada *intruder* (penyusup), karena penyusup (*intruder*) dengan IP 192.168.43.24 dan 192.168.43.24 masih bisa mengakses IP 192.168.43.24 bukti bahwa DoS masih terhubung pada *server* dan bukti bahwa *port scanning* masih terhubung pada *server*. Hasil dari pengujian setelah adanya serangan dapat dilihat pada Gambar 10.

Sumber: dokumen pribadi

Gambar 10. Hasil Pengujian Setelah Adanya Serangan



Sumber: dokumen pribadi

Gambar 11. Hasil Pengujian

Tabel 2. Pengujian Jaringan Akhir Sistem Keamanan *Honeypot*

No	OS	Proses Running		Keterangan
		Berhasil Masuk	Gagal Masuk	
1	*Spam*		√	*Spam* yang masuk sebenarny terperangkap di *Server Honeypot* da tercapture di *Server Honeypot.*
2	*Malware*		√	*Malware* yang masuk sebenarny terperangkap di *server honeypot* da tercapture di *server honeypot.*
3	*DdoS Attack*		√	Semua port yang terbuka denga sengaja agar DDoS *attack* menyerang *server honeypot*, buka *server* Asli.
4	*Scammer*		√	Di *Scammer*, semua *port* terlih terbuka, dan OS yang terlihat seolal olah itu adalah komputer *server* yar dengan sangat mudah dibobc padahal itu adalah *server honeypot*.
5	*Virus*		√	Masuknya segala metoc penyerangan yang menyulitka penyerangan menanam virus komputer *server*.

Dalam pengujian sistem keamanan jaringan berbasis *honeypot* yang perlu diperhatikan adalah penerapan keamanan jaringan tersebut untuk menjamin sumber data sistem yang dipergunakan dari serangan DDoS.

Analisis Sistem Keamanan Jaringan

Analisis sistem dilakukan untuk mengetahui kelebihan serta kekurangan dari rancangan sistem keamanan jaringan berbasis *honeypot* dibandingkan dengan sistem keamanan jaringan berbasis *firewall* yang dipakai sebelumnya. Selain itu juga akan dianalisis apakah sistem keamanan jaringan berbasis *honeypot* sudah berjalan sesuai dengan yang direncanakan sebelumnya.

Untuk memastikan sistem keamanan jaringan dapat berfungsi dan berjalan sesuai dengan yang diharapkan dari rancangan sistem keamanan jaringan tersebut, dilakukan pengujian kepada beberapa *client*. Dari pengujian sistem keamanan jaringan diperoleh data-data yang kemudian dari data tersebut akan dilakukan beberapa analisis terkait sistem keamanan jaringan lama dan sistem keamanan jaringan berbasis *honeypot*.

Analisis Serangan DDoS Terhadap Jaringan Awal

Berdasarkan data yang diperoleh dari hasil pengujian sistem keamanan jaringan awal, *firewall* tidak dapat melindungi *network* dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju *network* tersebut) lebih tepatnya tidak dapat melindungi dari serangan dengan metoda baru yang belum dikenal oleh *firewall*, dan juga tidak dapat melindungi dari serangan virus. Sedangkan data yang diberikan ke pihak lain untuk keperluan tertentu sering diketahui oleh pihak lain dan setelah ditelusuri bentuk serangan yang dilakukan pihak lain adalah usaha penyadapan dengan menggunakan program Nmap dan serta berusaha untuk masuk ke *port* yang terbuka. Gangguan keamanan komputer yang dialami PDAM Tirta AlBantani digolongkan dalam aspek privat (*privacy/confidentiality*). PDAM Tirta AlBantani masih memanfaatkan sistem keamanan melalui *firewall* dan anti *spyware*. Hal ini belum dapat mengatasi sabotase/pensurian data yang dilakukan oleh pihak tertentu karena tidak dapat menemukan pelaku penyerangan.

Analisis Serangan DDoS Terhadap *Honeypot*

Honeypot akan mendeteksi adanya seseorang yang memeriksa ke dalam jaringan saat melakukan *scanning port* karena pada *scan log honeypot* akan mencatat segala aktivitas yang dilakukan pada komputer *honeypot*. Pengujian data yang dilakukan berupa pengujian fungsionalitas interkoneksi *honeypot*, dimulai dari proses serangan dan pendeteksian serta penanganan serangan. Tampilan dari data yang dianalisis, kondisi sebelum dan sesudah penyerangan. Setelah melakukan berbagai proses dalam penerapan *honeypot*, terdapat kemudahan dalam penerapannya.

Dari hasil proses pengujian yang telah dilakukan adalah kondisi berjalan dengan baik pada saat sebelum terjadi penyerangan, kemudian terjadi gangguan saat serangan dilakukan, yang membuat pendeteksian menampilkan informasi dan rincian data dari penyerang, kemudian berhasil dilakukan penanganan dengan kondisi yang diperlukan sehingga semua serangan berhasil diblokir dengan baik. Untuk mengetahui seberapa aman tingkat keamanan yang telah diterapkan dalam sebuah jaringan *wireless*/nirkabel maupun kabel. Seperti yang diketahui tingkat keamanan bukan hanya berasal dari *hardware* dan *software* yang sudah ada namun peran penting dari pengguna yang melakukan konfigurasi dan dari perancangan jaringan itu sendiri.

V. PENUTUP

Kesimpulan

Dari semua langkah-langkah yang telah dilakukan dalam penelitian, maka dapat disimpulkan sebagai berikut:

1. Sistem *honeypot* telah berhasil meringankan tugas dari deteksi menjadi lebih sederhana, efektif dan murah. Konsepnya sendiri sangat mudah dipahami dan diimplementasikan. *Honeypot* sendiri ditujukan untuk mendeteksi serangan yang dilakukan oleh *attacker* dengan mengecoh *attacker* tersebut dengan fasilitas *mirror server*.
2. Sistem *honeypot* yang digunakan penulis merupakan *honeypots high interaction* dengan *rule sql injection* dan *denial of service* (DoS),

kedua *rule* tersebut bukanlah merupakan *rule* yang tergolong aman untuk sebuah sistem informasi yang besar, karena masih banyak tipe serangan yang bisa dilakukan oleh seorang *attacker*.

3. Berdasarkan dari analisis terhadap percobaan tersebut, terlihat bahwa *honeypot* memiliki kekurangan. Kekurangan terbesar berasal dari keterbatasan pandangan, karena sistem tersebut hanya menangkap aktivitas yang diarahkan pada sistem produk, dan tidak menangkap serangan pada sistem yang lain. Jika terdapat banyak *server* di *server farm* selain *server* tersebut diserang oleh *attacker*, maka serangan tersebut tidak dapat dideteksi oleh *honeypot*.

Saran

Berdasarkan uraiaan dari kesimpulan, maka kelebihan dan kekurangan di atas dapat menjadi pelajaran serta referensi untuk ke depannya. Saran-saran yang dapat dipertimbangkan untuk ke depan antara lain:

1. Dianjurkan melapisi sistem keamanan jaringan nirkabel dengan sistem *honeypot* khususnya untuk mendeteksi terhadap serangan dini.
2. Pengecekan jaringan berkala diperlukan untuk menghindari terjadinya permasalahan/*error* pada jaringan yang dapat menyebabkan kinerja jaringan menjadi lambat.

DAFTAR PUSTAKA

[1] Abdillah, Fauzi. (2015). "Konsep DoS dan DDoS (Distributed Denial of Service), serta Mekanisme Serangan DoS dan DdoS dan cara penanggulangannya." STMIK Dipanegara Makassar. Vol. 18. No. (2).

[2] Aridian, M dan Setiawan, Deris. (2012). "DoS dan DDoS dan cara Penanggulangannya." Jurnal Teknik Universitas Sriwijaya. Vol. 17. No. (5).

[3] Ariyus, Dony. (2007). "Intrusion Detection System". Yogyakarta: Andi Yogyakarta.

[4] Candra, Setia Bayu. (2013) "Analisis Penerapan Jaringan Keamanan Menggunakan IDS dan Honeypot." Jurnal Ilmu Komputer Universitas Dian Nuswantoro Semarang. Vol. 12. No. (9)

[5] Ferdiansyah, Doddy. (2013). "Pemanfaatan Teknologi Honeypot Dalam Meningkatkan Availability Pada Sistem Jaringan." Jurnal Teknik Universitas Pasundan. Volume 15 Nomor (1).

[6] Hermawan, Rudi. (2012). "Analisis Konsep dan Cara Kerja Serangan Komputer DDoS." Jurnal Teknik Informatika Universitas Indraprasta PGRI: Jakarta. Vol. 21. No. (10).

[7] Ikhwan, Syariful dan Elfitri. (2014). "Analisa Delay yang Terjadi Pada Penerapan Demilitarized Zone (DMZ) Terhadap Server Universitas Andalas." Jurnal Teknik Informatika Universitas Andalas. Vol. 3. No. (2).

[8] Linto. (2009). "Pengantar Jaringan Komputer." Penerbit: Andi publisher.

[9] Masdian. (2012). "Implementasi dan Analisa HIDS (Host Intrusion Detection System) dengan Snort untuk mencegah DDoS (Distributed Denial of Service)." Jurnal Teknik Informatika Universitas Trunojoyo Bangkalan. Vol. 121. No. (25).

[10] Muhammad, Faris. (2010). "Analisis Serangan DDoS pada Server Ubuntu yang beroperasi dalam Wireless Local Area Network." Jurnal elektro dan komunikasi institute teknologi Telkom Bandung. Vol. 5. No. (9).

[11] Nur, Khasanah. (2008). "Metode pencegahan serangan Denial of Services." Jurnal Universitas Sriwijaya. Vol. 34. No.(10).

[12] Nurwenda S, et al. (2004) "Analisis Kelakuan Denial of Service attack (DoS attack) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas,"Jurnal UNIKOM. Vol. 7. No. (3).

[13] Prasetyo, Dimas (2011) "Perancangan Kolaborasi Sistem Deteksi Intruksi Jaringan Tersebar dengan Honeypot menggunakan Metode elert Correlation." E-journal Teknik Elektro dan Komputer UNSRAT Manado. Vol. 3. No. (2).

[14] Randy, Mentang, et al. (2015) "Perancangan dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System." E-journal Teknik Elektro dan Komputer UNSRAT Manado. Volume 5. No (7).

[15] Rafiudin, Rahmat. (2010). "Mengganyang Hacker dengan Snort." Penerbit: Andi Publisher

[16] Setiawan, Thomas. (2004). "Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal." Jurnal Institut Teknologi Bandung. Vol. 11. No. (6).

[17] Sopandi, Dede (2010). "Instalasi dan Konfigurasi Jaringan Komputer." Bandung:Penerbit Informatika

[18] Sumarno, dan Bisosro, Sabto. (2003). "Solusi Network Security dari Ancaman SQLInjection dan Denial of Service (DOS)." Jurnal Teknik Universitas Muhammadiyah Sidoarjo. Vol. 5. No. (28)

[19] Syafrizal, Melwin. (2005). "Pengantar Jaringan Komputer." Yogyakarta: Andi Yogyakarta

[20] Utdirartatmo, Firrar. (2005). "Trik Menjebak Hacker Dengan Honeypot" Yogyakarta: Andi Publisher.

[21] Zamrudiah, M. (2009). "Analisa Mekanisme Pertahanan DoS dan DDoS pada Virtual Machine dengan menggunakan IDS Center." Jurnal Universitas Indonesia. Volume 13. No. (2).

[22] Zulkarnaen, Disky. (2010) "Implementasi Honeypot Sebagai Alat Bantu Deteksi Keamanan Jaringan Pada Kantor Pengawasan dan Pelayanan Bea dan Cukai Tipe A2 Palembang" Jurnal Teknik Informatika STMIK PalComTech Palembang. Volume 4, No (13).